The Information Commissioner's Response to the Proposals for Revising the Code of Practice for Victims of Crime Consultation

The Information Commissioner is responsible for promoting and enforcing data protection law in the UK including the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018). She is independent of government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. She does this by providing guidance to individuals and organisations, solving problems where she can, and taking appropriate action where the law is broken. She welcomes the opportunity to respond to this consultation.

Many of the consultation questions fall outside of the scope of the Information Commissioner's regulatory role as they are directed towards organisations with expertise in working with victims of crime directly. For this reason, key data protection points are addressed below rather than by responding directly to each of the questions in turn.

The Information Commissioner recognises the importance of revising the Code of Practice for Victims of Crime (VCOP) and the need to strengthen the provisions available for victims. Consideration must be given to the relevant data protection requirements to ensure that data is processed appropriately and that the changes to data protection legislation are reflected in the revised Code.

Changes in legislation

The current VCOP is dated October 2015 and the drafting of the original Code was conducted under the former Data Protection Act 1998. With the introduction of the GDPR and DPA 2018 last year, changes are required to bring the VCOP in line with the new data protection legislation in order to avoid confusion for practitioners. Therefore in response to the first consultation question, data protection requirements should be a focus for the second consultation.

Lawful basis for processing

When processing personal data, organisations require a lawful basis for processing. Data controllers will need to consider which data protection regime the processing falls under, and to document the appropriate lawful basis. The scenarios outlined in the VCOP may fall under GDPR or Part 3 of the DPA 2018 depending on the circumstances, and therefore consideration of the requirements under both sets of legislations need to be taken.

When a competent authority is processing personal data for criminal law enforcement purposes, it will need to adhere to Part 3 of the DPA 2018.[1] As the first point of contact for victims of crime is often the police, the initial collection of some victim data may fall under this legislation. Part 3 requires that the processing of personal data meets the requirements set out in section 35 whereby amongst other things, the processing must be based on law.[2]

Where it is determined that the processing relevant to the VCOP falls under the GDPR, an article 6 lawful basis for processing will be required, where special category data is processed, an article 9 special category condition will also be necessary. Data regarding criminal convictions and offences may be processed under these circumstances and in these instances, an article 10 condition will be need to be identified.[3]

Consent

The current VCOP 2015 references 'consent' and states that police officers are required to 'explain to all victims that their details will be passed to victim support services unless they ask the police not to'. The code continues to state that 'explicit consent' must be sought from victims of the most serious offences before sending their details to support services. The reference to consent poses certain data protection issues which will need addressing in the revised VCOP. Consideration will also need to be taken of the processing of data relating to children and it is worth highlighting that children have the same data rights as adults.

The references above imply that consent is currently the lawful basis relied upon for the obtaining and sharing of victim data with support services. However it is important to clarify that consenting to take up the provision of a service is not the same as relying on consent for the sharing of personal data. There is a difference between the provisions which allow a data

[1] The law enforcement purposes are defined in section 31 of the DPA 2018 as 'The prevention, investigation detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.'

[2] In the event of sensitive processing, Section 35 refers to the requirement to obtain consent, or a Schedule 8 condition must be met. Under these circumstances, an appropriate policy document should be produced and where a Schedule 8 condition is relied upon, the processing must be strictly necessary for the law enforcement purpose.

[3] A schedule 1 condition under the DPA 2018 will also be necessary when relying on an article 10 condition and will be required in certain circumstances when processing sensitive data under article 9

controller to share certain information with a particular agency, and an individual agreeing to take up these particular services. This needs clarification in the revised VCOP.

Under the new data protection regime, there have been notable changes surrounding the threshold for consent. Consent must be opt-in, not opt-out and an 'opt-out' will not be seen as offering a genuine choice. It is also not clear why it currently stands that certain categories of victims are required to provide explicit consent, whilst there was an opt-out option for other victims. We understand that the new code proposes to group the three categories of victims eligible for enhanced entitlements into a single category called 'victims with the greatest needs'. If it is intended to process their data in a different way, the rationale and lawful basis needs to be documented.

There is reference in the VCOP 2015 and also in the proposals to refer victims to specialist services "where appropriate and available". Further clarification and guidance for practitioners regarding what is meant by this statement in terms of data sharing is necessary so that practitioners can be explicitly clear when a referral can be made. With regards to referring "where available", it is important to note that in terms of data protection, consent needs to be specific and informed. Amongst other things, this means that practitioners would need to detail any third party agencies data will be shared with when consent is obtained.

The Independent Victims' Commissioner for London's Review of Compliance with the Victims' Code of Practice states that a significant issue raised by response officers was the need to obtain 'explicit' consent from victims for a referral to a support service since the introduction of GDPR. In some cases, officers were making difficult judgement calls on whether or not to refer, this echoes our own engagement on the issue.

It is also worth referencing the HM Government Victims Strategy which states that some of the changes to the Victims' Code will be to 'provide clearer information on how victims' personal data will be shared between agencies and support services with clear explanations of how victims may opt-in or out'. We welcome this statement, however it is important to reinforce that in terms of data protection, consent must be opt-in only.

The GDPR also gives a specific right to withdraw consent. If you cannot offer a genuine choice or it is impossible for it to be freely given, fully informed or withdrawable, then consent is not appropriate.[4] If you would still process/disclose the personal data without consent, asking for consent

[4] Although 'consent' is not defined in Part 3 of the DPA 2018, recital 35 of the Law Enforcement Directive refers to the consent of the data subject as defined in Regulation (EU) 2016/679 (the GDPR). From this, it can be inferred that the standard of consent under Part 3 of the DPA 2018 aligns with the definition of consent under GDPR.

is misleading and inherently unfair as it presents the individual with a false choice and only the illusion of control.

Consent will not usually be appropriate where the controller is in a position of power over the individual, for example public authorities. Controllers would need to look carefully at the particular circumstances of the processing and demonstrate that the individual really does have a free choice to give or to refuse consent. If the high bar for consent cannot be achieved, then it is worth considering another more appropriate lawful basis for processing. Our detailed guidance on consent should be considered when revising the VCOP.

The Victims Strategy reinforces that many victims who are entitled to enhanced services are not always getting the right support. We consider that the confusion around consent may be a contributing factor. The revised VCOP should ensure that there is no confusion between the lawful basis for sharing personal data with support services, and the decision by victims to take up the services offered.

Data Protection should not be a barrier to sharing information when it is necessary to do so. Further clarity should be provided to practitioners so that it is clear when relevant data can be shared between agencies in the circumstances set out in the VCOP. The suggestion set out in question 2: 'to have separate guidance alongside the Code aimed at victims and practitioners' may be a useful way of clarifying these issues.

Privacy information

The Information Commissioner acknowledges the challenges faced by front line staff to clearly explain, and for victims to understand, the support and information they should receive at every stage of their journey. The HM Government Victims Strategy reports that only one third of participating victims had been told about the VCOP and their entitlements.

The requirement to provide privacy information to individuals in relation to how their data will be processed is a fundamental right under data protection legislation. This is an obligation that data controllers will need to comply with regardless of the lawful basis for processing (unless a restriction applies) and data should not be processed in a way which victims would not reasonably expect.

It is often most effective to provide privacy information to individuals using a combination of different techniques, including layering. Careful consideration should be taken regarding which format is the most appropriate under the circumstances, the provision of this information can be adapted to how information is collected. The vulnerability of victims should be factored when providing privacy information to determine

whether there are risks in providing information in a particular format. The Information Commissioner acknowledges the dedicated gov.uk page and the 'pledge card' referred to in the proposal and recommends that the ICO guidance on privacy information be adhered to in order to ensure that individuals are fully aware of how their data will be processed.

Victim Personal Statements

The consultation raises concerns that few victims are aware of how their Victim Personal Statement (VPS) will be used in court and also that the statement is disclosed to the defence and may be reported in the media. This also links to the requirement to provide privacy information and is particularly important in these circumstances. Steps should therefore be taken to ensure that clear and effective privacy information is also provided to victims in relation to how they can expect data contained within their VPS to be used.

We acknowledge that the Independent Victims' Commissioner for London's Review of Compliance with the Victims' Code of Practice raises concerns that there is often a lack of privacy when the VPS is made. The Victims Strategy suggests using new technology such as body-worn cameras in order to give victims more choice about how they give their statement. In these circumstances, appropriate data protection considerations should be given to the sensitivity of the data and how victims may provide their statement in a way that is appropriate and secure.

Further consideration needs to be given to ensuring the processing is done in a more privacy friendly way, and it is not clear how recording victims will achieve this. If the statements may be recorded, victims need to be made aware of how the recording will be used. In these circumstances the relevant privacy requirements relating to body-worn cameras should be considered and we would recommend reviewing our CCTV code of practice (please note that this guidance is being updated).

In response to question 8, 'do you agree that victims should be provided with a copy of their Victim Personal Statement', it is worth noting that victims are likely to be entitled to receive this information through the subject access provisions. As there is a route to access this information, it may be more open and transparent to provide victims with a copy of their statement at the outset.

Data Sharing

The Information Commissioner acknowledges concerns about re-traumatising victims where individuals are referred to different agencies and are being asked to take part in several needs assessments throughout

the criminal justice process as information is not always passed between agencies and support services.

Data protection is sometimes wrongly cited as a barrier to data sharing, instead it should be viewed as a framework of safeguards to ensure fair, lawful and proportionate data sharing. The Information Commissioner recognises that a multi-agency approach can be an effective way of helping victims of crime, and there are data protection obligations that organisations must adhere to when conducting multi-agency data sharing. Having appropriate data sharing arrangement in place will help to reduce the risk of victims being re-traumatised by having to repeat information to various agencies which relates to question 14 in the consultation proposal.

The Information Commissioner is currently updating her Data Sharing Code of Practice (the code) to reflect changes in data protection legislation; it will also explain new developments to take into consideration. The Code has recently been published for consultation. The aim is for the code to be laid before Parliament and become statutory later in the year. Due regard should be given to the code when developing a multi-agency approach to services and data sharing.

Adhering to the code will help to ensure good practice around data sharing and help to manage risks associated with sharing large volumes of sensitive data. Following the code and adopting its practical recommendations will help to give organisations confidence to collect and share personal data in a way that is fair, transparent where appropriate and in line with the rights and expectations of the people whose information is being shared.

We also acknowledge the proposal of Victim Liaison Officers or a Single Point of Contact in order to provide victims with relevant information in a timely manner. It is important that these officers are familiar with data protection and receive appropriate training. The suggestion of improving guidance for these officers is welcomed and should include appropriate data protection considerations.

Creating local accountability – Police and Crime Commissioners

The role of Police and Crime Commissioners (PCCs) outlined in the proposal are acknowledged. Whilst their specific data processing responsibilities have not been defined, consideration needs to be taken to determine whether their function will include the processing of personal data.

With regards to the role of PCCs through local criminal justice partnerships, consideration is required regarding the relationship between the relevant bodies. This includes whether the organisations are considered as joint controllers or controller / processors. Joint controllers must consider who will take primary responsibility for complying with the data protection

obligations. Each party must have a clear understanding of where their responsibilities start and end, data sharing agreements will assist with this. Joint controllers will have to agree an arrangement under article 26 of the GDPR where they set out these terms. Contracts should be in place where it is determined that the relationship is that of data controller / processor, under these circumstances it would be the controllers who determine the means and purposes of the processing.

The Information Commissioner would be happy to provide further advice on the matter if needed.

Information Commissioner

9 September 2019 V1.0